Polityka bezpieczeństwa danych osobowych

Polityka bezpieczeństwa przetwarzania danych osobowych

w stowarzyszeniu AVSI POLSKA z siedzibą w Warszawie,

Rozdział 1

Postanowienia ogólne

§ 1

Celem Polityki bezpieczeństwa przetwarzania danych osobowych w AVSI POLSKA zwanej dalej „Polityką bezpieczeństwa", jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych sposobu przetwarzania informacji zawierających dane osobowe.

§ 2

Polityka bezpieczeństwa została utworzona w związku z wymaganiami zawartymi w rozporządzeniu Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. oraz w ustawie z 10 maja 2018 r. o ochronie danych osobowych.

§ 3

Ochrona danych osobowych realizowana jest poprzez zabezpieczenia fizyczne, organizacyjne, oprogramowanie systemowe, aplikacje oraz użytkowników.

Dla skutecznej realizacji Polityki bezpieczeństwa administrator danych osobowych zapewnia:

a) Odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne;

b) Kontrolę i nadzór nad Przetwarzaniem danych osobowych;

c) Monitorowanie zastosowanych środków ochrony.

§ 4

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w AVSI POLSKA rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) integralność systemu – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
   5) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
   6) zarządzanie ryzykiem – rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

§ 5

1. Administratorem danych osobowych przetwarzanych w AVSI POLSKA jest Zarząd.

Rozdział 2

Definicje

§ 6

Przez użyte w Polityce bezpieczeństwa określenia należy rozumieć:

1) ustawa – rozumie się przez to ustawę z 10 maja 2018 r. o ochronie danych osobowych (tekst jedn.: Dz.U. z 2018 r. poz. 1000);
2) rozporządzenie – rozporządzenie Parlamentu Europejskiego i Rady (UE) z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych
3) dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
4) zbiór danych osobowych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
5) przetwarzanie danych – rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
6) system informatyczny – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
7) system tradycyjny – rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji i wyposażenia, i środków trwałych w celu przetwarzania danych osobowych na papierze;
8) zabezpieczenie danych w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
9) administrator systemu informatycznego – rozumie się przez to osobę lub osoby, upoważnione przez administratora danych osobowych do administrowania i zarządzania systemami informatycznymi;
10) użytkownik – rozumie się przez to upoważnionego przez administratora danych osobowych lub administratora bezpieczeństwa informacji (o ile został powołany), wyznaczonego do przetwarzania danych osobowych pracownika;

11) identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
12) hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Rozdział 3

ZAKRES STOSOWANIA

§ 7

1. W AVSI POLSKA przetwarzane są w szczególności dane osobowe pracowników oraz klientów (w tym kontrahentów, pracowników, współpracowników, członków organów, klientów) zebrane w zbiorach danych osobowych.
2. Informacje te są przetwarzane zarówno w postaci dokumentacji tradycyjnej, jak i elektronicznej.
3. Polityka bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.
4. Administrator danych osobowych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób. W przypadku planowania takiego działania Administrator danych osobowych wykona czynności określone w art. 35 i n. RODO.
5. Administrator danych osobowych prowadzi rejestr czynności przetwarzania, którego wzór stanowi Załącznik do niniejszej Polityki.

§ 8

Politykę bezpieczeństwa stosuje się w szczególności do:

1) danych osobowych przetwarzanych w systemie: Comarch ERP XL, Comarch ERP Optima, Płatnik, Microsoft Office, Office 365;
2) wszystkich informacji dotyczących danych klientów (w tym kontrahentów, pracowników, współpracowników, członków organów, klientów) oraz pracowników;
3) wszystkich danych klientów (w tym kontrahentów, pracowników, współpracowników, członków organów, klientów) oraz pracowników;
4) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
5) rejestru osób dopuszczonych do przetwarzania danych osobowych;
6) innych dokumentów zawierających dane osobowe.

§ 9

1. Zakresy ochrony danych osobowych określone przez dokumenty Polityki bezpieczeństwa mają zastosowanie do systemów informatycznych, w których są przetwarzane dane osobowe, a w szczególności do:
   a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;
   b) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
   c) wszystkich pracowników, współpracowników i innych osób mających dostęp do informacji podlegających ochronie.
2. Do stosowania zasad określonych przez dokumenty Polityki bezpieczeństwa, ścisłego przestrzegania zakresu nadanego upoważnienia, przetwarzania danych i ochrony danych osobowych zgodnie z przepisami, zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu zobowiązani są wszyscy pracownicy, współpracownicy oraz inne osoby mające dostęp do informacji podlegających ochronie.
3. Administrator danych osobowych zapewnia w szczególności, aby:

a) pracownicy lub współpracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków;

b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z Upoważnieniem do przetwarzania danych osobowych – wzór Upoważnienia stanowi załącznik do niniejszej Polityki.

c) każdy pracownik/współpracownik zobowiązał się do zachowania danych osobowych przetwarzanych w AVSI POLSKA w tajemnicy – oświadczenie stanowi element Upoważnienia do przetwarzania danych osobowych.

Rozdział 4

Wykaz zbiorów danych osobowych

§ 10

1 . Dane osobowe gromadzone są w zbiorach:

1) Akta osobowe pracowników
2) Listy płac pracowników;
3) Lista płac klientów
4) Deklaracje ubezpieczeniowe pracowników i dane przesyłane do ZUS
5) Dane współpracowników
6) Zbiór upoważnień
7) Dane zleceniobiorców
8) Dokumenty archiwalne
9) Umowy zawierane z klientami/darczyńcami/beneficjentami
10) Dokumenty firmowe, statutowe – AVSI POLSKA

11) Poczta e-mail
12) Newsletter
13) Zbiór dokumentów rekrutacyjnych

§ 11

Zbiory danych osobowych wymienione w § 10 ust. 1 pkt 1,3,7-12 podlegają przetwarzaniu w sposób tradycyjny oprócz zbiorów określonych w pkt 2,3-6,13, które gromadzone są i przetwarzane przy użyciu systemu informatycznego.

Rozdział 5

Wykaz budynków, pomieszczeń i stref do przetwarzania danych osobowych

§ 12

1. Dane osobowe przetwarzane są w budynku, mieszczącym się w AVSI POLSKA przy ulicy Flory 9/2 w Warszawie 00-586.

2. Załącznik nr 1

Rozdział 6

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

§ 13

Załącznik nr 2

Rozdział 7

STRUKTURA ZBIORÓW DANYCH WSKAZUJĄCYCH ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH

§ 14

Struktura zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych dla programów i systemów stosowanych w AVSI POLSKA przedstawia się w sposób następujący:

Załącznik nr 3

Rozdział 8

SPOSÓB PRZEPŁYWU DANYCH MIĘDZY POSZCZEGÓLNYMI SYSTEMAMI I WSPÓŁPRACY SYSTEMÓW INFORMATYCZNYCH ZE ZBIORAMI DANYCH

§ 15

Przepływ danych pomiędzy poszczególnymi systemami

Załącznik nr 4

Rozdział 9

Środki techniczne i organizacyjne zabezpieczenia danych osobowych

§ 16

1. Zabezpieczenia organizacyjne
    1) sporządzono i wdrożono Politykę bezpieczeństwa;
    2) sporządzono i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
    3) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych bądź osobę przez niego upoważnioną;
    4) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
    5) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
    6) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
    7) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
    8) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
    9) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
2. Zabezpieczenia techniczne
    1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą ROUTER z wbudowaną funkcjonalnością firewall
    2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
    3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania w komputerach stacjonarnych oraz w przypadku komputerów przenośnych dodatkowo hasłem zabezpieczającym dysk twardy za pomocą szyfrowania przed odczytaniem danych

4) Wykorzystywanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe.

3. Środki ochrony fizycznej:
   1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest przez firmę ochroniarską,
   2) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
   3) urządzenia służące do przetwarzania danych osobowych znajdują się w zamykanych pomieszczeniach.

Rozdział 10

ZADANIA INFORMATYKA

§ 18

1. Informatyk odpowiedzialny jest za:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego
   2) optymalizację wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego
   3) instalacje i konfiguracje oprogramowania systemowego, sieciowego
   4) konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz zabezpieczającym dane chronione przed nieupoważnionym dostępem
   5) nadzór nad zapewnieniem awaryjnego zasilania dla urządzeń tego wymagających mających wpływ na bezpieczeństwo przetwarzania danych
   6) współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego
   7) zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego
   8) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie
   9) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji

10) przyznawanie na wniosek osób do tego upoważnionych ściśle określonych praw dostępu do informacji w danym systemie
11) zarządzanie licencjami, procedurami ich dotyczącymi
12) prowadzenie profilaktyki antywirusowej

2. Praca informatyka jest nadzorowana pod względem przestrzegania ustawy o ochronie danych osobowych, rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz Polityki bezpieczeństwa przez administratora danych lub administratora bezpieczeństwa informacji.

Rozdział 11

SZKOLENIA UŻYTKOWNIKÓW

§ 20

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u administratora danych osobowych, a także o zobowiązaniu się do ich przestrzegania.
3. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych.
4. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

Rozdział 12

Powierzenie przetwarzania danych osobowych

1. Administrator danych osobowych może powierzyć przetwarzanie danych osobowych, innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO.
2. Przed powierzeniem przetwarzania danych osobowych, Administrator danych osobowych w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

Rozdział 13

POSTANOWIENIA KOŃCOWE

§ 21

1. Administrator danych osobowych ma obowiązek zapoznać z treścią Polityki każdego użytkownika.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
5. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości

wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

6. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy ustawy oraz rozporządzenia.